Statement of Dr. Linda Wilbanks
Chief Information Officer
National Nuclear Security Administration
U.S. Department of Energy
Before the
Committee on Energy & Commerce
Subcommittee on Oversight & Investigations

January 30, 2007

Thank you for the opportunity to discuss the cyber security incident at the Los Alamos National Laboratory (LANL) and the actions the National Nuclear Security Administration (NNSA) has taken to prevent similar incidents at other NNSA sites. We have a very important national security mission and take these responsibilities very seriously.

Within the NNSA, the Chief Information Officer reports directly to Mr. Michael Kane, the Associate Administrator for Management and Administration. As the CIO, I am responsible for information technology within NNSA. I came to NNSA after almost three years as the CIO at Goddard Space Flight Center, NASA. I have over 30 years experience in information technology with a bachelors degree in Mathematics, a Masters degree in Engineering, and a Ph.D. in Computer Science. My office works with the Department of Energy (DOE) CIO, Mr. Tom Pyke, and the NNSA sites to develop and implement appropriate cyber security policies.

NNSA is dependent on information and upon the systems that create, process, store, and communicate information to carry out its national security mission. We must guard against a wide range of attacks from the sophisticated outsider who wishes to break into our cyber infrastructure as well as the accidental or malicious insider. As the NNSA CIO, I am responsible to the NNSA Administrator for cyber security, specifically policies and procedures to ensure the security of the information and technology as it relates to the NNSA mission, and to enhance NNSA's ability to protect NNSA's classified, sensitive and unclassified information and systems.

I would like to provide the Members of the Committee additional information relative to actions the NNSA has taken in response to the recent LANL incident. I will then address actions specific to LANL and those actions taken across the complex.

When the most recent incident was reported, the NNSA Cyber Security Program Manager and the Director of the Diskless Workstation Taskforce immediately flew to Los Alamos with two members of the Department of Energy's (DOE) cyber security team. Their objective was to learn as much as possible about the incident from the cyber perspective and determine if any of the contributing factors could put LANL or other sites at risk. In November, I flew to Los Alamos myself and spoke with both Federal and contractor cyber security personnel, who are responsible for the computer systems at Los Alamos, including the system in question.

At Los Alamos we found was that there was a cyber security plan in place for the system signed by the Designated Approving Authority (DAA) who is located at the Federal Site Office. However, upon review following the incident, my office believed that the plan was too generic and did not address specific risks to that system. For example, the plan stated that the cages containing the servers did not have to be locked as they were contained within a Vault Type Room and only authorized personnel were allowed in the room. The plan also allowed for scanning and for a printer to be connected to the classified systems even though there was no justified need to print. The server in question had accessible USB ports on the front and back that were not visible to the cyber security person in the room. These conditions allowed the subject in question to download classified data to her personal thumb drive. In order to move data to or from any of the servers, a password was needed. The subject in question only had the password to the server dedicated for scanning purposes, which was her assigned duty. This prevented her from accessing any information other than what she had been cleared to scan. We have since secured all USB ports at all NNSA sites and are reviewing all cyber security plans to ensure they address the specific risks for that system. This type of incident, the undetected transfer of classified information to a portable device, could no longer occur at any NNSA site.

We have undertaken a number of actions in response to the recent incident at LANL to prevent this type of incident and strengthen the cyber security:

- The DAA from the Sandia Site Office has been detailed to LANL to strengthen the Federal cyber security oversight and inspection capabilities.

- Additional funding was provided to the Site Office to hire three contractors to support the DAA and cyber security activities. These contractors will be separate from the Laboratory contract.

- At the request of the Los Alamos Deputy Site Office Manager my office sent a team of seven cyber security experts from HQ and NNSA sites to inspect the vaults to determine if they were in compliance with the Department's directive to close ports. The on-the-ground team was able to verify that the lab was not in full compliance and because of that process we were able to initiate corrective measures. A team of federal cyber security experts went back to LANL on January 22 to re-evaluate the lab's efforts for compliance. The initial reports from this second team are positive and indicate LANL has corrected the deficiencies previously identified.

During the past year, NNSA has made changes to strengthen the cyber security posture of the complex and more recently addressed issues identified by the LANL incident.

- In early 2006 a Designated Approving Authority (DAA) official was appointed to work at each site. The DAA's sole responsibility is dedicated to cyber security for their site. Prior to this change one person was responsible for many systems at several sites. This resulted in cyber security plans that were more generic, that did not address specific risks and incorporated minimal, if any site inspections being done to verify the system was following the plan. A dedicated DAA at each site will mitigate this vulnerability.

- Since a contributing factor to the incident at LANL was the generic cyber security plan, the Site DAAs that have now been assigned to all sites are currently reviewing all system cyber security plans to ensure these plans address the specific risks of each system. This review will identify plans that may be generic and allow peripherals that are not required (i.e., printers) or insufficient security, (i.e., unlocked cages) or any other omission or lack of specifics in the plan such as those identified in the LANL vault security plan. A standard template for a cyber security plan has been distributed to ensure all plans contain the critical information required to thoroughly asses the risks associated with operating an IT system. Each site is responsible for making the plan specific for each system, and removing weaknesses.

- In July, the NNSA Forensics Facility, Information Assurance Response Center (IARC) was assigned the responsibility for compiling all NNSA cyber security incidents and reporting them within the specified time periods to the Department's cyber security incident response center. All Sites, instead of having to report incidences to multiple places, now report them only to the IARC. This ensures the correct reporting of cyber security incidents and allows NNSA to track and analyze incidents, which will result in better risk identification and overall cyber management. This comprehensive information has already provided us with valuable lessons on areas that need to be strengthened across

NNSA.

- In November 2006, as a result of the Los Alamos incident, we required all sites to identify all open ports on classified systems, and determine whether they needed to be open or could be permanently closed. We found that three sites had already identified this as a risk and were working on closure or had already closed the ports. (Deputy Secretary Clay Sell later issued a memo to implement this action for all of DOE by January 15, 2007.) We also purchased an enterprise license for software to monitor open port activity, an action that was in progress when the incident occurred. We have evidence that these actions are successfully working. On January 17, a personal thumb drive was inserted into a classified machine to upload work. The software successfully prevented the information from being uploaded to the classified machine and notified the system administrator.

- My office has worked with the DOE CIO, Mr. Pyke, to identify areas where policies and procedures are needed to strengthen cyber security guidance and to issue them in a timely manner. Those new policies included establishing a governance framework (Departmental Cyber Security Management) and establishing baseline cyber security controls for national security (classified) information systems (National Security System Controls Manual).

- We have set up a schedule for my office to inspect the cyber security implementation at all NNSA sites. Those inspections will start in February and conclude in April. Each inspection will last for one week. The inspection team will consist of two HQ cyber security personnel and a cyber security professional from another site. These inspections will occur annually and strengthen Site office oversight. They will also serve as refresher training for the DAA on what they should be inspecting at their sites.

Cyber security programs are direct funded activities within Safeguards and Security line of the NNSA Weapons Activities appropriation. Funding allocation decisions are based on enterprise priorities and site risks. After my office identifies the risks and balances priorities for program initiatives, the Administrator takes the information into consideration with similar information from all other NNSA programs and makes overall resource allocation decisions across NNSA. In the current year, due to additional requirements placed on the sites in order to comply with the new policies and procedures, my office has reprioritized ongoing activities and reallocated $6M to cover these extra activities at the sites, of which $1.05M went to LANL.

NNSA is responsible for over 70 percent of the classified networks within the Department. We take this responsibility very seriously and have made maintaining the security of the classified networks our highest priority to ensure there are no breaches. The Department is on schedule with the implementation of diskless workstation project, and completion is scheduled for September 30, 2008. NNSA fully supports the Department of Energy’s federated approach to cyber security that is directed in the recently updated Departmental order on Cyber Security Management, 205.1A. We are jointly working with the Department to maximize our efforts and resources to ensure a secure environment for the transmission and storage of our information.

Mr. Chairman, NNSA is working very diligently to maintain a secure environment for our information and that of the Department. We work closely with our sites to identify the risks and we work closely with DOE to maximize our resources. We are moving ahead in many areas and we are making progress.